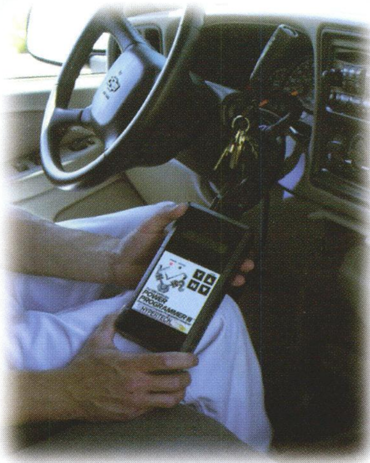
الغــش المعلومــاتــي

د. محمد سامي الشوا*

في شهر سبتمبر عام ١٩٨٣م وتحت عنوان «ميلاد نزعة» نشرت مجلة «EXPertises» الفرنسية وقائع حادثة تتلخص في أن عامل طلاء مباني قد توجه إلى أحد البنوك لإيداع شيك خاص به وتزامن ذلك لحظة فصل الموزع الآلي للنقود حيث شاهد مستخدم صيانة الأجهزة الآلية وهو يقوم باستخراج نقود البنك من الآلة «عند الطلب» عن طريق استخدام بطاقة خاصة وقد أحدث هذا الابتكار للآلة تصدعاً في الحياة العادية لعامل الطلاء ، وحرص هذا الأخير على التدرب على تقنية الحاسب الآلي لمدة عامين ثم قام بالسطو على صانع الموزعات الآلية وتمكن بفضل الآلة المسروقة من التوصل إلى أسلوب كيفية السحب لكنه لم يتمكن من الاستفادة مما تتوصل إليه فقد ألقي عليه القبض ونسبت إليه جريمة سرقة الآلة.





يجب أن نقرر ـ علاوة على ذلك ـ أن هناك العديد من الأمثلة وحالات العجز التقني التي تترك الفرصة لمشيدي برامج الحاسب الآلي لاقتراف أفعال الغش المعلوماتي.

ودائماً ما يوضع في الاعتبار دقة الأسلوب أكثر من فعل الغش نفسه. ويميل مرتكبو أفعال الغش المعلوماتي إلى إظهار تفوقهم ومستوى براعتهم، لدرجة أنه إزاء ظهور أي تقنية مستحدثة فإن مرتكبي أفعال الغش الذين لديهم شغف بالآلة، يحاولون إيجاد «وغالباً ما يجدون» الوسيلة إلى تحطيمها.

والجدير بالملاحظة، أن بعض مرتكبي أفعال الغش المعلوماتي، ليسوا على جانب كبير من الخطورة الإجرامية، وهم يكتفون في العادة بتحقيق انتصارات تقنية، دون أن تكون لهم نوايا آثمة.

وهناك بواعث أخرى، غالباً ما تكون آثمة وغير شريفة، تحض على ارتكاب أفعال الغش المعلوماتي، وهي على قدر كبير من الخطورة بالنسبة

لسير أو انتظام المنشأة أو النظام المشتبه فيه.

وإن الرغبة في تحقيق الثراء الشخصي، هي الدافع إلى الغش الأكثر انتشاراً ويبدو ذلك جلياً من خلال تحقيق أجرته إحدى المجلات المتخصصة بخصوص موضوع «الأمن المعلوماتي»، ومن خلال ما ذكره السيد parker يتضح أن:

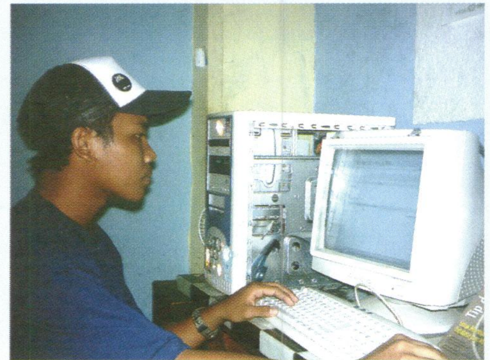
«٤٣٪ من حالات الغش المعلن عنها، قد تمت ممارستها من أجل اختلاس الأموال.

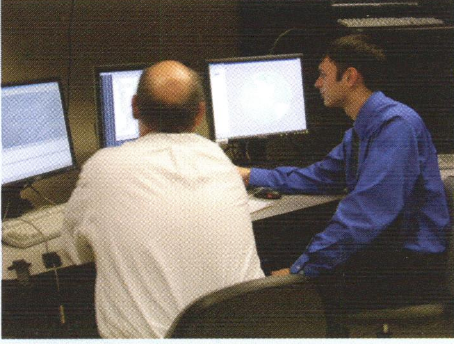
٢٣٪ من أجل سرقة المعلومات.

١٩٪ أفعال الإتلاف.

١٥٪ سرقة وقت الآلة أي الاستعمال غير المشروع للحاسب الآلي لأجل تحقيق أغراض شخصية».

وفي الواقع، فإن المحرك لاقتراف فعل الغش المعلوماتي، يمكن أن ينطلق من مجرد النجاة من غرق الديون المستحقة، أو من المشاكل العائلية الراجعة إلى النقود، أو من الخسائر الضخمة لألعاب القمار، أو من إدمان المخدرات وقد تكون جميع الوسائل بالنسبة للبعض مشروعة في هذه المرحلة فالغاية تبرر الوسيلة ولذا فإن بيع المعلومات المختلسة هو نشاط متسع للغاية ويمكن أن نذكر في هذا الشأن واقعة استيلاء مبرمج لدى إحدى الشركات الألمانية على اثنين وعشرين شريطاً يحتوي معلومات مهمة بخصوص العملاء وإنتاج الشركة وقد هدد السارق ببيعها للشركات المنافسة مالم تدفع له فدية مقدارها مائتا ألف دولار (٢٠٠,٠٠٠) وقد قامت الشركة بتحليل الموقف، وفضلت دفع المبلغ من أجل استرداد الشرائط المغنطة المسروقة حيث قدرت أن الخسائر التي يمكن أن تنشأ عن إفشاء محتواها تفوق بكثير المبلغ المطلوب.





وهناك مثال آخر خاص بمجموعة من رجال شرطة دلاس الأمريكية، حيث تمكنوا بواسطة التلاعب في برنامج الحاسب الآلي الموجود في حوزتهم، والمختزن فيه محاضر الشرطة، من إسقاط بعض الغرامات المستحقة مقابل مبلغ من المال.

وقد دفعت الرغبة بمستخدم يعمل لدى إحدى شركات التأمين كي يحتفظ بوظيفته التي سبق أن فصل منها، إلى أن يحتجز الذاكرة المركزية للحاسب الآلي الخاص بالشركة.

وقد هدد المختلس رئيسه في العمل، بأنه إذا حاول أن يلغي بطاقة أجرته من ذاكرة الحاسب الآلي، فإن هذه الأخيرة سوف تدمر تلقائياً عن طريق ما يعرف بالقنبلة المنطقية.

ويمكننا أن نلاحظ، ومن ثم أن نستنتج من مجرد حصر أفعال الغش المعلوماتي، أن الأمل في تحقيق الربح هو السبب الأساسي الذي يسيطر على هذه الأفعال ونستطيع أن نقرر أيضاً احتفاظ البنوك وشركات التأمين بقائمة من أفعال التعدي المعلوماتي التي ليست لها في نفسها قيمة معتبرة سوى تقوية ومعالجة أنظمتها المعلوماتية.

ومما هو مؤكد أن الإنسان مخلوق هش من الناحية السيكولوجية، حيث يمكن في بعض المواقف أن يستسلم للمؤثرات الخارجية، أو أن يكون قد فرض عليه سلوكه المخادع بدافع من الإكراه أو الحقد.

وقد دفع الانتقام في هذا الخصوص بمحاسب شاب، إلى أن يتلاعب بالبرامج المعلوماتية حيث إنه بعد مضي عدة أشهر من رحيله من المنشأة التي يعمل بها، تختفي كل البيانات الحسابية الخاصة بديون هذه المنشأة.

وقد أمكن الكشف في بعض المواقف الأخرى، على أن مجرد إظهار شعور جنون العظمة، هو الدافع لارتكاب فعل الغش المعلوماتي وفي هذا الشأن نجد المحلل أو المبرمج المعلوماتي وهو مفتاح سر كل نظام وقد ينتابه إحساس بالإهمال أو النقص داخل المنشأة التي يعمل بها.

وقد يندفع تحت تأثير رغبة قوية من أجل تأكيد قدراته التقنية لإدارة المنشأة إلى ارتكاب فعل الغش المعلوماتي وقد يعترف به، ومن ثم يجد ترضية من خلال الإفصاح عن شخصيته أمام العامة.

وتمارس أفعال الغش المعلوماتي - والتي تنفذ تحت تأثير تهديد أو ضغط من الغير - في بعض مجالات الأعمال التجارية وعلى وجه

الخصوص في نطاق المنافسة والتجسس.

وقد تدفع الحاجة إلى توفير سنوات عديدة من البحث وتجنباً لاستثمار الملايين التي تتكلفها عملية البحث العلمي، نقول تدفع هذه الحاجة بعض المنشآت بل بعض الدول إلى الاتصال بالأفراد الذين يشغلون مراكز مرموقة ويعملون لصالح منشآت أخرى منافسة بهدف الاطلاع على بعض المعلومات الأساسية، وتستخدم أساليب عديدة للوصول إلى الهدف المنشود أو المعلومات المشتهى فيها، وأكثرها شيوعاً الرشوة، الإغراء، الخداع، وعند اللزوم الإقناع المقترن بالإكراه أو التهديد بإفشاء نقاط الضعف لدى الفرد المعني.

ولا يكتفى في بعض المجالات والتي تبدو على قدر كبير من الحساسية، بمجرد الاتصال، بل يفضلون زرع جواسيس خصيصاً لذلك، ونذكر في هذا الخصوص واقعة موظف يعمل بأحد مكاتب شركة مشهورة متعددة الجنسيات ومركزها إحدى مدن ألمانيا الغربية «قبل توحيدها» حيث كان يتمتع هذا الموظف بسمعة طيبة لدى كل المنشآت العميلة وقد لوحظ عقب اختفائه، أن هذا الموظف المثالي كان يعمل في الحقيقة في مجموعة جواسيس أنشئت خصيصاً في ألمانيا الغربية من أجل مهاجمة أنظمتها المعلوماتية وقد نجح هذا الجاسوس في أن ينقل إلى ألمانيا الشرقية معلومات مهمة بخصوص ثمانية آلاف منشأة تعمل في ألمانيا الغربية ولكن يجب الاعتراف بأن هذا الجاسوس كان ضحية لعملية ابتزاز.

ولا شك أن الشخص المسؤول عن المركز المعلوماتي، هو بدون منازع في وضع يمكنه من استغلال نقاط الضعف المحتملة لمركز المعالجة وتعد الألفة المتبادلة بينه وبين الأنشطة التي يزاولها ومركز الثقة الذي يحوزه أفضل أسلحة له لارتكاب أفعال الغش المعلوماتي.

ولا يجب أن نغض الطرف، عن أن أحد التهديدات العظمى التي تؤثر في الأنظمة المعلوماتية، هو أن يعهد بكل مسؤولية المركز إلى شخص واحد بمفرده فقد تدفع هذه الثقة العمياء لمحللي ومبرمجي الحاسب الآلي. وتتلخص وقائعه في أن مستشاراً لدى أحد البنوك الكبرى كان يتمتع بثقة مطلقة من جانب هذا البنك. وقد سمحت اختصاصاته بالولوج في مفاتيح إلكترونيين من ثلاثة أساسية للتحكم في التحويل الإلكتروني للنقود من بنك إلى بنك آخر وقد تمكن بفضل قدراته في مجال



المعالجة الآلية للمعلومات وتآلفها الشديد مع النظام المعلوماتي من الوصول إلى المفتاح الثالث، واستطاع أن ينقل في الحال عشرة ملايين دولار إلى حساب بنكي فتح باسمه في سويسرا وقد ألقي القبض عليه وصدر ضده حكم بالسجن ست سنوات.

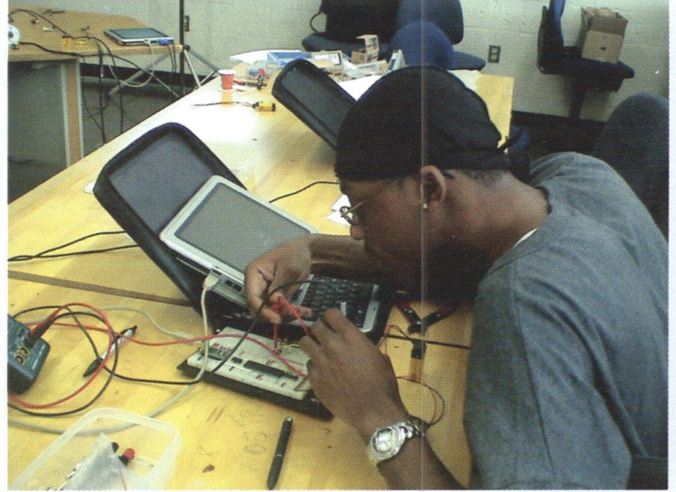
وهناك جانب آخر من المسؤولين عن الأنظمة المعلوماتية، استفادوا من مواقف خاصة وأحداث جديدة من أجل ارتكاب أفعالهم الآثمة: كحالة رعب في مركز المعالجة، أو الذعر المصطنع أو احتجاز المعاملات عن طريق إحداث إشباع أو مجرد استغلال أزمة في المنشأة «كتغيير الإدارة على سبيل المثال» ولكن على كل حال، يجب ألا نغض الطرف، عن أن التسامح والتساهل الذي يهيمن دائماً على تطبيق إجراءات المراقبة وممارسة التفتيش، يعد من العوامل التي تساعد على تضخم أفعال الغش المعلوماتي.

وفي النهاية، فإن الهدف الأساسي للتعرف على شخصية مرتكبي أفعال الغش المعلوماتي الذين ينتمون إلى الجيل الجديد هو الاقتناع بأن أفضل حماية، تبدأ دائماً بالمعرفة الجيدة والكاملة للعدو المنتظر.

وعند حديثنا عن المجني عليه في الجريمة المعلوماتية نشير إلى أنه وفقاً لتقدير بعض خبراء الصندوق الدولي للبنوك f.b.I فإنه من المستحيل أن تحدد على نحو دقيق نطاق الجرائم المعلوماتية.

ولا يعلم ضحايا هذه الجرائم شيئاً عنها إلا عندما تكون أنظمتم المعلوماتية هدفاً لفعل الغش، وحتى عندما يعلمون، فهم يفضلون عدم إفشاء الفعل فلا يوجد من يريد الاعتراف بانتهاك نظامه المعلوماتي.

وعلى الرغم من ذلك فقد استطاع اتحاد



البنوك في جنيف، أن يقدر خسائر أوروبا الغربية من ظاهرة الغش المعلوماتي حيث بلغت حوالي أربعة وخمسين مليون فرنك فرنسي في عام ١٩٨٨م كما قدرت خسائر الاقتصاد الأمريكي الناشئة عن هذه الظاهرة بحوالي أربعمائة مليون دولار وفقاً لما أشار إليه التقرير.

وتشير الإحصاءات النادرة في هذا المجال إلى أن جميع الأنشطة التي تستخدم الحاسب الآلي تكون عرضة لخطر ظاهرة الغش المعلوماتي، فأي قطاع من الأنشطة ليس بمنأى عن ذلك ويبدو بجلاء أن انتهاك هذه الأنظمة المعلوماتية هو الأكثر توفيراً بالنسبة للمحتالين. ويلاحظ مع ذلك، أن الاتجاه الأساسي للغش المعلوماتي، يستهدف البنوك. ووفقاً لتحقيق باشرته إحدى المجلات المتخصصة فقد تبين أن:

١٩٪ من أفعال الغش المعلوماتي تستهدف البنوك.

١٦٪ للإدارة.

١٠٪ للإنتاج الصناعي.

١٠ ٪ للمعلومات.

ثم يلي ذلك شركات التأمين والشركات الخاصة ويستهدف الغش المعلوماتي في الحقيقة المنشآت المالية، أو على الأقل تلك التي تهيمن على القيم الرأسمالية. ومن جهة أخرى، فإن المعلومات هي إحدى المصالح الأساسية المستهدفة بعد النقود وأصبحت منذ الآن فصاعداً هي المنفذ إلى اقتصاد السوق وقد شيدت على أساسها صناعة حقيقية ومتطورة. ولقد نما إلى جوار «السوق الشرعي للمعلومات» «السوق السوداء للمعلومات» وفيه تتم مقايضة وبيع المعلومات المسروقة، أو المقتبسة من أصحابها الحقيقيين والشرعيين ويرتبط هذا النوع من الإجرام إذن بالجزء الأعظم للأنشطة الاقتصادية والاجتماعية للمجتمع - ويمكن تصوره بالنسبة للمعلومات الآتية:

أ - المعلومات المالية:

حيث تمس هذه الظاهرة المركز الحسابي والإداري وتنقلات الأموال والاستثمارات سواء في المنشآت العامة أو الخاصة.

ب - المعلومات التجارية والصناعية:

حيث تستهدف هذه الظاهرة الدراسات الخاصة بالأسواق ومشروعات الاستثمار والتصنيع والإنتاج والتجارة والتوزيع والأسعار ومراكز البيع والقطاع الصناعي للإنتاج.

جـ المعلومات الشخصية:

وهي تلك المختزنة في ذاكرات الحاسبات الآلية للبنوك وشركات التأمين ولدى المحامين والمستشفيات وأقسام الشرطة والأحزاب والنقابات وقد تهدد هذه الاعتداءات مباشرة قدسية وسرية الحياة الخاصة أو الحرية النقابية والسياسية... إلخ.

وإذا كان عقاب أفعال الغش المعلوماتي مازال محدوداً جداً إلى الآن فمرد ذلك إلى أسباب عديدة: بعضها فني والآخر قانوني والثالث إنساني.

وفي الواقع، فإن التقنية العالية التي تتسم بها هذه الظاهرة، هي إحدى العقبات الأساسية في اكتشاف الأفعال غير المشروعة التي تنشأ عنها وهذا ما يفسر أن جزءاً صغيراً من أفعال الغش هو الذي تم اكتشافه وعلاوة على ذلك فإن الصدفة وحدها هي التي لعبت دوراً في كشف الغالبية العظمى من الحالات المكتشفة.

وعلاوة على ذلك، وعلى فرض اكتشاف فعل من أفعال الغش المعلوماتي تثور هنا مشكلة أخرى خاصة بالإثبات المادي لفعل الغش والمسؤولية المحتملة لهؤلاء الذين لهم حق الإشراف على المركز المستهدف، وهل لهم الصلاحيات اللازمة من أجل تطبيق وتنظيم مراعاة تعليمات الأمن؟ وهل لديهم السلطات اللازمة لإمكان التقدير ووضع التنظيمات الضرورية في حالة حدوث أضرار ناشئة عن إفشاء معلومات على قدر من الحساسية. ولا يمكن من جهة أخرى تقدير نطاق أفعال الغش المعلوماتي، وذلك بسبب ردود الأفعال السلبية لضحايا هذه الأفعال ويبقى سكوت وسلبية هؤلاء الضحايا خير معين لمرتكبي هذه الأفعال.

* كلية الحقوق - جامعة المنوفية - مصر ■